ANDERSINNO

Verkko-ostoksesi turvana

4.2.2014

Tuomas Suutari

Kuka? Mikä?

Tuomas Suutari

Ohjelmistoarkkitehti Anders Innolla

Anders Inno

Verkkoliiketoimintaan erikoistunut ohjelmistotalo

www.andersinno.fi

Tietoturva-asioilla ei tarvitse aina pelotella

Maksaminen ja luottokorttitiedot

- Maksettaessa pankkien verkkotilisiirtojen tai luottokorttiyhtiöiden palveluiden kautta luottokortin numero ei päädy kauppiaalle
- PCI DSS -tietoturvastandardi
  - Määrittelee tietoturvavaatimukset maksukorttien tietoja käsitteleville tahoille. Sisältä mm.:
    - Suojaa tallennetut kortinhaltijatiedot
    - Siirrä kortinhaltijoiden tiedot ja muut luottamukselliset tiedot julkisissa tietoverkoissa salattuina
    - Kehitä turvallisia järjestelmiä ja sovelluksia sekä ylläpidä niitä
- Postiennakko

Salasanat

- Vastuuntuntoinen palveluntarjoaja ei tallenna salasanoja
- Salasanojen sijaan tallennetaan todennuskoodi, jolla salasana voidaan tarkistaa
- Oikein toteutettuna todennuskoodista ei voi päätellä salasanaa
  - Tällöin salasanasi ovat turvassa vaikka käyttäjätiedot päätyisivät ulkopuolisen käsiin

Verkkopankkien erityissuojaukset

- Avainlukulistat
  - Luvut täysin satunnaisia
  - Riittää, että pidät avainlukulistan hyvässä tallessa
- Tekstiviestivarmistukset

SSL-suojaus

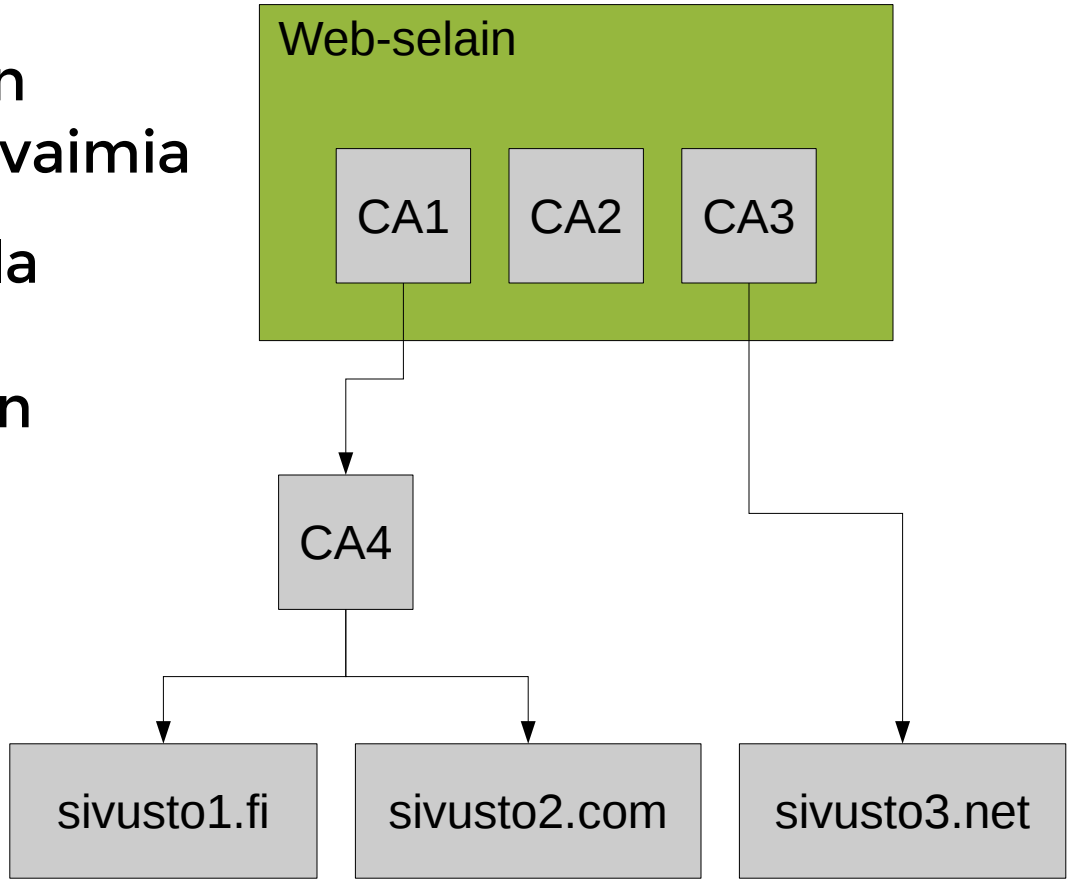
- SSL = Secure Sockets Layer
- Uudempi nimi: TLS = Transport Layer Security
- Suojaa Internet-liikennettä (pankkiyhteydet, sähköposti, jne.)
  - Salaa siirrettävät tiedot
  - Varmistaa palvelimen luotettavuuden (allekirjoitus)
- Yleisin käyttökohde on WWW-sivujen HTTPS-protokolla
- Perustuu julkisen avaimen salaukseen

Julkisen avaimen salaus

- Käytetään avainparia:
  - Yksityinen ja julkinen avain
- Julkisella avaimella voidaan luoda viestejä, jotka voidaan lukea ainoastaan yksityisellä avaimella
- Yksityisellä avaimella voidaan luoda allekirjoitus, jonka voi tarkistaa julkisella avaimella
- Allekirjoittamalla julkisia avaimia voidaan luoda luotettujen avaimien hierarkia

Luotettujen avaimien hierarkia

- Web-selaimessa on joukko luotettuja avaimia
- Luotetulla avaimella allekirjoitettuun avaimeen luotetaan



RSA-salaus

- Tunnetuin julkisen avaimen salausmenetelmä
- Perustuu suurien alkulukujen tekijöihin jakamisen vaikeuteen
- Esimerkki: Julkisessa avaimessa on luku n = p*q = 189045759400521368590761780337832778 92742520347440315684326 97. Mitkä ovat kokonaisluvut p ja q?
  - Vastaus: 11111111111111111111111 (23 ykköstä) ja $2^{127}-1$ (eli 170141183460469231731687303715884105727).
- SSL-yhteyksissä käytetyissä avaimissa luku n on yleensä pituudeltaan kymmenkertainen (2048 bittiä)

Kysymyksiä?

Kiitos!